

WE CLAIM:

1. A method for multiplying an elliptic curve point $Q(x,y)$ by a scalar to provide a point kQ , the method comprising the steps of:
 - 5 a) selecting an elliptic curve over a finite field F such that there exists an endomorphism ψ where $\psi(Q) = \lambda \cdot Q$ for all points $Q(x,y)$ on the elliptic curve, and λ is an integer,
 - b) establishing a representation of said scalar k as a combination of components k_i and said integer λ
 - 10 c) combining said representation and said point Q to form a composite representation of a multiple corresponding to kQ and
 - d) computing a value corresponding to said point kQ from said composite representation of kQ .
2. A method according to claim 1 wherein each of said components k_i is shorter than said scalar k .
3. A method according to claim 1 wherein said components k_i are initially selected and subsequently combined to provide said scalar k .
4. A method according to claim 1 wherein said representation is of the form
$$k_i = \sum_{l=0}^{i-1} k_l \lambda^l \text{ mod } n$$
 where n is the number of points on the elliptic curve.
5. A method according to claim 4 wherein said representation is of the form $k_0 + k_1$.
- 20 6. A method according to claim 1 wherein said scalar k has a predetermined value and said components k .
7. A method according to claim 3 wherein said value of said multiple kQ is calculated using simultaneous multiple addition.
8. A method according to claim 7 wherein grouped terms G_l utilized in said simultaneous multiple addition are precomputed.
- 25

25

- d) establishing for each of said representations a window having a width less than the length of each of said representations;
- e) initiating a sequential examination of said representations by said windows to obtain a position for one of said windows in one of said representations containing a respective one of said combinations in said table;
- f) retrieving from said table the one of said point multiples corresponding to said respective one of said signed bit combinations in said table to obtain therefrom one of said portions;
- g) accumulating said portion and continuing examination of said representations with a doubling of said accumulator for each bit-wise shift of said windows to obtain a representation of said coordinate of said point kP in said accumulator.

13. A method according to claim 12, wherein one of said respective points is derived from said initial point P and one of said components using an endomorphism of said curve.
14. A method according to claim 13, wherein said portions of said one of said respective points are derived from portions of the other of said respective points using said endomorphism.
15. A method according to claim 12, wherein one of said respective points is derived from said initial point P, one of said components, and a private key.
16. A method according to claim 15, wherein said portions of said respective points are precomputed and stored in said table.